UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/035,526	11/09/2001	Konrad Wrona	53806-00003USPX	4663

27045 7590 04/29/2005

ERICSSON INC.
6300 LEGACY DRIVE
M/S EVR C11
PLANO, TX 75024

EXAMINER	
ANANTHANARAYANAN, RAMYA	

ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 04/29/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/035,526	WRONA ET AL.	
	Examiner	Art Unit	
	Ramya Ananthanarayanan	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 November 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

1. Claims 1-25 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

3. The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1-23 and 25 are rejected under 35 U.S.C. 102(e) as being anticipate by Zolotorev et al. (U.S. Patent 6,859,795).

5. With respect to claim 1, Zolotorev et al. disclose a method of returning change to a payer in an electronic payment system wherein a due amount is paid by a payer to a payee via a first payment certificate having a value of a first amount higher than a due amount, the method comprising:

Receiving, by a payment provider, of the first payment certificate (column 22, lines 29-50);

Verifying, by the payment provider, of the first payment certificate (column 22, lines 29-50);

Crediting, by the payment provider, of the due amount to the payee (column 22, lines 29-50);

Determining, by the payer, of at least one change return value such that the sum of the determined at least one change return value is equal to a difference between the first amount and the due amount (column 22, lines 51-61);

Generating, by the payer, of at least one change return certificate according to the at least one change return value (column 22, lines 51-61);

Blinding, by the payer, of the change return certificate (column 11, lines 22-32);

Generating, by the payer, of a first signature by signing the blinded change return certificate (column 11, lines 22-32);

Sending, by the payer, of a message comprising the first signature to the payee (column 11, lines 19-21);

Forwarding, by the payer, of the message to the payment provider (column 12, lines 33-67);

Verifying, by the payment provider, of the first signature (column 12, lines 33-67);

Verifying, by the payment provider, of a change return value indicated by the message (column 12, lines 33-67);

Generating, by the payment provider, of a blinded second signature by signing the blinded change return certificate if the verification of the first signature and of the change return value is successful (column 11, lines 22-32);

Forwarding, by the payment provider, of the blinded second signature to the payer (column 11, lines 22-32);

Unblinding, by the payer, of the blinded second signature (column 21, lines 66-67 to column 22, lines 1-13);

Verifying, by the payer, of the second signature (column 21, lines 66-67 to column 22, lines 1-13);

Forming, by the payer, of at least one second payment certificate by linking the change return certificate and the unblinded second signature (column 22, lines 51-61).

6. With respect to claim 2, Zolotorev et al. disclose a method, further comprising:

Assigning, by the payment provider, of a second asymmetric key pair comprising a second public key and a second private key to a change return value (column 19, lines 12-15);

Blinding, by the payer, of the change return certificate via a blinding factor, the blinding factor being encrypted via the second public key (column 21, lines 18-29);

Generating, by the payment provider, of the blinded second signature by signing the blinded change return certificate via the second secret key (column 21, lines 18-29);

Wherein the step of unblinding of the blinded second signature by the payer comprises a division of the blinded second signature by the blinding factor (column 21, lines 66-67 to column 22, lines 1-13);

Wherein the step of verifying the second signature by the payer comprises a decryption of the unblinded second signature and a test of whether the decrypted unblinded second signature corresponds to a generated change return certificate (column 21, lines 66-67 to column 22, lines 1-13).

7. With respect to claim 3, Zolotorev et al. disclose a method, wherein the payment provider sends the second public key to the payee and the payee forwards the second public key to the payer (column 19, lines 21-40).

8. With respect to claim 4, Zolotorev et al. disclose a method of performing tasks of a payment provider in a change returning transaction in an electronic payment system, wherein a payment provider receives a first payment certificate having a value of a first amount higher than the due amount and verifies the first payment certificate and credits the due amount to a payee, the method comprising:

Receiving a message comprising a first signature of a blinded change return certificate (column 12, lines 33-67);

Verifying the first signature (column 12, lines 33-67);

Verifying a change return value indicated by the message (column 12, lines 33-67);

Generating a blinded second signature by signing the blinded change return certificate if the verification of the first signature and of the change return value is successful (column 11, lines 22-32); and

Sending the second signature to the payee (column 22, lines 51-61).

9. With respect to claim 5, Zolotorev et al. disclose a method, wherein:

A second asymmetric key pair comprising a second public key and a second private key is assigned by the payment provider to the change return value (column 19, lines 12-15);

The change return certificate is blinded by means of a blinding factor encrypted via the second public key (column 21, lines 18-29); and

The blinded second signature is generated by the payment provider by signing the blinded change return certificate by means of the second secret key (column 21, lines 18-29).

10. With respect to claim 6, Zolotorev et al. disclose a method, wherein the message comprising the first signature includes the first payment certificate in order to perform crediting of the first amount (column 22, line 55).

11. With respect to claim 7, Zolotorev et al. disclose a method, wherein:

A first asymmetric key pair comprising a first public key and a first private key is assigned to the first payment certificate (column 20, lines 4-30);

The first payment certificate comprises the first public key (column 20, lines 4-30);

The first signature is generated by the payer via the first private key (column 20, lines 4-30); and

The verification of the first signature is performed by the payment provider via the first public key (column 20, lines 4-30).

12. With respect to claim 8, Zolotorev et al. disclose a method, wherein:

The first signature indicates the value of the first amount of the first payment certificate (column 20, lines 4-30); and

The payment provider verifies the value of the first amount of the first payment certificate (column 20, lines 4-30).

13. With respect to claim 9, Zolotorev et al. disclose a method, wherein the payment provider stores at least one of the first signature and the message comprising the first signature (column 20, lines 4-10).

14. With respect to claim 10, Zolotorev et al. disclose a method of performing tasks of a payer in a change returning transaction in an electronic payment system wherein the payer pays a due amount by means of a first payment certificate having a value of a first amount higher than the due amount, the method comprising:

Determining at least one change return value such that the sum of the determined change return values is equal to a difference of the first amount and the due amount (column 22, lines 51-61);

Generating at least one change return certificate according to the at least one change return value (column 11, lines 22-32);

Blinding the change return certificate (column 11, lines 22-32);

Generating a first signature by signing the blinded change return certificate (column 11, lines 22-32);

Sending a message comprising the first signature to a payee (column 11, lines 19-21);

Receiving a blinded second signature comprising a signed blinded change return certificate (column 11, lines 22-32);

Unblinding the blinded second signature (column 21, lines 66-67 to column 22, lines 1-13);

Verifying the second signature (column 21, lines 66-67 to column 22, lines 1-13); and Forming at least one second payment certificate by linking the change return certificate and the unblinded second signature (column 22, lines 51-61).

15. With respect to claim 11, Zolotorev et al. disclose a method wherein:

A first asymmetric key pair comprising a first public key and a first private key is assigned to the first payment certificate (column 20, lines 4-30);

The first payment certificate comprises the first public key (column 20, lines 4-30);

The first signature is generated by means of the first private key (column 20, lines 4-30).

16. With respect to claim 12, Zolotorev et al. disclose a method, wherein

A second asymmetric key pair comprising a second public key and a second private key is assigned to a change return value (column 19, lines 12-15);

The change return certificate is blinded by means of a blinding factor encrypted by means of the second public key (column 21, lines 18-29);

The unblinding of the blinding second signature comprises a division of the second signature by the blinding factor (column 21, lines 66-67 to column 22, lines 1-13);

The verification of the second signature comprises the decryption of the unblinded second signature and a test of whether the decrypted unblinded second signature corresponds to a generated change return certificate (column 21, lines 66-67 to column 22, lines 1-13).

17. With respect to claim 13, Zolotorev et al. disclose a method, wherein the first signature indicates the value of the first amount of the first payment certificate (column 20, lines 4-30).

18. With respect to claim 14, Zolotorev et al. disclose a method, further comprising receiving the second public key (column 19, lines 12-15).

19. With respect to claim 15, Zolotorev et al. disclose a method, wherein at least one of the second payment certificate and a private key corresponding to the second payment certificate is sent to a third party for storing as a backup (column 3, lines 4-5).

20. With respect to claim 16, Zolotorev et al. disclose a method, wherein the first signature is generated by signing the blinded change return certificate and a change return value linked to the blinded change return certificate (column 22, lines 51-61).

21. With respect to claim 17, Zolotorev et al. disclose a method, wherein the message comprises at least one of the blinded change return certificate and the change return value corresponding to the blinded change return certificate (column 11, lines 22-32).

22. With respect to claim 18, Zolotorev et al. disclose a method, wherein the first payment certificate comprises a macropayment certificate (Abstract).

23. With respect to claim 19, Zolotorev et al. disclose a method, wherein the first payment certificate comprises a micropayment certificate (Abstract).

24. With respect to claim 20, Zolotorev et al. disclose a method, wherein the blinding of the change return certificate comprises building a digest of the change return certificate and blinding the digest (column 21, lines 59-65).

25. With respect to claim 21, Zolotorev et al. disclose a method, wherein the message comprising the first signature includes the first payment certificate in order to perform the payment of the first amount (column 20, lines 4-30).

26. With respect to claim 22, Zolotorev et al. disclose an article of manufacture for returning change to a payer in an electronic payment system, wherein a due amount is paid by a payer to a payee via a first payment certificate having a value of a first amount higher than a due amount, the article of manufacture comprising:

At least one computer readable medium (column 15, lines 35-55);

Processor instructions contained on the at least one computer readable medium (column 15, lines 35-55: It is inherent in a computing device such as a personal computer to have a processor), the processor instructions configured to be readable from the at least one computer

readable medium by at least one processor and thereby cause the at least one processor to operate as to:

Receive the first payment certificate (column 22, lines 29-50);

Verify the first payment certificate (column 22, lines 29-50); and

Credit the due amount to the payee (column 22, lines 29-50);

Wherein the payer determines at least one change return value such that the sum of the determined at least one change return value is equal to a difference between the first amount and the due amount (column 22, lines 51-61););

Wherein the payer blinds the change return certificate (column 22, lines 51-61),

Wherein the payer generates a first signature by signing the blinded change return certificate (column 22, lines 51-61);

Wherein the payer sends a message comprising the first signature to the payee (column 11, lines 19-21);

Wherein the payer forwards the message to the payment provider (column 12, lines 33-67);

The processor instructions being further configured to be readable from the at least one computer readable medium by the at least one processor and thereby cause the at least one processor to operate as to:

Verify the first signature (column 12, lines 33-67);

Verify a change return value indicated by the message (column 12, lines 33-67);

Generate a blinded second signature by signing the blinded change return certificate if the verification of the first signature and of the change return value is successful (column 11, lines 22-32); and

Forward the blinded second signature to the payer (column 11, lines 22-32);

Wherein the payer unblinds the blinded second signature (column 21, lines 66-67 to column 22, lines 1-13);

Wherein the payer verifies the second signature (column 21, lines 66-67 to column 22, lines 1-13); and

Wherein the payer forms at least one second payment certificate by linking the change return certificate and the unblinded second signature (column 22, lines 51-61).

27. With respect to claim 23, Zolotorev et al. disclose a payment device comprising:

Means for determining at least one change return value such that the sum of the determined at least one change return value is equal to a difference of a first amount and a due amount (column 22, lines 51-61););

Means for generating at least one change return certificate according to the at least one change return value (column 22, lines 51-61);

Wherein the payer generates at least one change return certificate according to the at least one change return value (column 22, lines 51-61);

Means for blinding the change return certificate (column 22, lines 51-61);

Means for generating a first signature by signing the blinded change return certificate (column 22, lines 51-61);

Means for sending a message comprising the first signature to a payee (column 11, lines 19-21);

Means for unblinding a blinded second signature comprising a signed blinded change return certificate (column 21, lines 66-67 to column 22, lines 1-13);

Means for verifying the second signature (column 21, lines 66-67 to column 22, lines 1-13); and

Means for forming at least one second payment certificate by linking the change return certificate and the unblinded second signature (column 22, lines 51-61).

28. With respect to claim 25, Zolotorev et al. disclose a bank device adapted to perform tasks of a payment provider in a change returning transaction in an electronic payment system, the bank device comprising:

Means for receiving a message comprising a first signature of a blinded change return certificate (column 20, lines 4-30);

Means for verifying the first signature (column 20, lines 4-30);

Means for verifying a change return value indicated by the message (column 20, lines 4-37);

Means for generating a blinded second signature by signing the blinded change return certificate if the verification of the first signature and of the change return value is successful (column 11, lines 22-32); and

Means for sending the second signature to the payee (column 11, lines 22-32).

Claim Rejections - 35 USC § 103

29. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

30. Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over Zolotorev et al. (U.S. Patent 6,589,795) in view of Blaze et al. (U.S. Patent 6,789,068).

31. Zolotorev et al. and Blaze et al. are analogous art because both are in the field of electronic commerce.

32. With respect to claim 24, Zolotorev et al. disclose the limitations of claim 23, upon which claim 24 is dependent. Zolotorev et al. do not disclose an article, wherein the payment device comprises a mobile phone.

Blaze et al. disclose an article, wherein the payment device comprises a mobile phone (column 2, lines 45-47).

33. It would have been obvious to one of ordinary skill in the art at the time of the invention to have combined the teachings of Blaze et al. with the teachings of Zolotorev et al. in order to integrate with existing billing systems and devices (column 2, lines 45-47).

Conclusion

34. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. U.S. Patent 4,949,380 to Chaum et al. and the Brickell et al. publication "Trustee-based Tracing Extensions to Anonymous Cash and the making of Anonymous Change" (1995) address some of the limitations presented in the claims of the instant application.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ramya Ananthanarayanan whose telephone number is (571) 272-5860. The examiner can normally be reached on Monday through Friday, 8:30 -5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

RA

AU2131
4/17/05